Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 165 – 171

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Establishment of Light Weight Cryptography for Resource Constraint Environment using FPGA

Chanthini Baskar[a], Balasubramaniyan C[b], Manivannan D[a,b,]*

[a]*School of computing SASTRA University, Thanjavur,613401, Tamil Nadu, India*
[b]*School of computing SASTRA University, Thanjavur,613401, Tamil Nadu, India*

Abstract

Wireless Sensor Networks (WSN) is the accumulation of large number of tiny, low power autonomous devices. By the very nature, WSN are prone to attack and difficult to secure, manage, even for most savvy network administrators. Security algorithms are requisite for protecting data transmission in WSN, since unlicensed wireless bandwidth is used for data communication. In this work a lightweight encryption algorithm with modified key generation by fusing logistic map and tent map is proposed and the same is implemented in ALTERA DE1 cyclone II FPGA which occupies only 1550 logic element for 128 bit key size and a maximum throughput of 200 Kbps is achieved.

Peer-review under responsibility of organizing committee of the ICISP2015

*Keywords:*Light weight encryption, FPGA, Chaotic map, WSN;

1. Introduction:

Wireless sensor networks (WSN) are widely deployed to monitor real time environmental parameters such as temperature, pressure, humidity, sound, etc. and to transfer the collected data wirelessly to a base station or sink node. The exploitation of WSN made it suitable even for safety critical and mission critical applications such as surveillance maintenance and battlefield monitoring. Sensor nodes are autonomous devices which operates on the battery, are highly power constrained.Power plays a major role in the sensor node efficiency, performance, nodes

* Corresponding author. Tel.: +91-04362-264101-106 (ext 3618).
*E-mail address:*dmv@cse.sastra.edu

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.027

lifetime and security parameters.

As the WSN is infrastructure less ad hoc network, which can be deployed anywhere immediately under any cause of critical requirement such as disaster rescue operations, battlefield surveillance during any fulminant situation. Security is the prime factor for consideration in any mission critical requirement, where implementing strong cryptographic algorithms into the sensor node is not possible because of its resource constrained nature. To overcome this security issues light weight cryptographic algorithms were developed and proven to be secure for mobile devices. Though they are secure, their security level is not sufficient for utilizing them in the critical applications. Also the latest developments in modern digital electronics, embedded systems, wireless communications techniques have paved way for the improvement of lightweight, portable, handheld devices such as mobiles, PLDs, laptops, sensor networks and so on. These devices are highly resource and power constrained. Implementing highly secure algorithms in resource constrained devices will deplete the power by increasing computational complexity. Thus, the need for lightweight cryptography arises. There should always be a tradeoff between the security and resource utilization while implementing them in real time devices.

Traditional cryptographic algorithms are proven to be secure in critical applications with large number rounds for encryption and decryption of the data. The key is more important in any cryptographic algorithm, where it is the parameter on which security level of any algorithm depends on an algorithm states the methodology for computing the key with confidential data. Key generation part of an algorithm should be designed carefully in order to ensure the security of any system and it consumes more computational steps for strong key without any correlation with the next generated key value. However to increase the randomness of the key is very important to ensure the strength of the algorithm. In the literature many key generation schemes specific for wireless sensor networks are derived and implemented.

Key management is another important task in WSN, where the generated key can be distributed and managed using many techniques such as pairwise key distribution; matrix based key distribution and so on. But the size of the key is very important in the energy constrained sensor networks. Large key size ensures the randomness, but proportionally increases the network load with complexity. This in turns consumes more power storing and transmitting larger keys in the network for encryption. Session wise key generation is a technique used for highly secured applications, where storing of key is not advised. These session keys should be generated at particular time when required, hence time and condition based key generation is important in sensor networks.

In this paper a light weight cryptographic algorithm with minimum computation with a chaotic map based key generation scheme is proposed and implemented in the Field Programmable Gate Array (FPGA). Its performance is analyzed by encrypting the sensor data and compared with other lightweight algorithms in literature. Power analysis of the proposed algorithm is performed and tabulated. The paper is organized as section 2 describes work related to lightweight cryptography in literature and section 3 describes the methodology and key generation. In section 4 results are analyzed and compared with other work and finally section 5 gives the concluding remarks and future directions.

2. Related work:

Cryptography algorithms in the literature generally deal with the block cipher and stream cipher. The stream cipher is more likely to be preferred in the modern encryption as the software process the series of data and block cipher is mainly used in any hardware base encryption, especially in the parallel processing architectures. In [1] author has depicted the clearly about the stream cipher and how it is computed and key stream produces for stream ciphering. The XOR function is between the plain text and key. Blowfish is well known private key lightweight encryption algorithm used modern electronics. According to the latest literature it is used in computers and mobile application with 1088 slices [2]. Camelia [3] is a lightweight encryption algorithm used with 128 and 256 bit key length and 1025 slices in FPGA. CAST 128 and CAST 256 both follow the same structure, where they are symmetric algorithm used for encryption with large logic element utilization of about 5052 CLBs [4] [5].

CURUPIRA I is specially proposed for lightweight encryption in the sensor networks and mobile devices [6]. It uses the NAND gate implementation in FPGA and performs well in a resource constrained environment. GOST is another algorithm proposed by the Russian government in 1989 and according to recent literature low power implementation of 650 GE is presented by the author [7]. LUCIFER is the predecessor of DES and implemented by the IBM in 1971 uses a key size of 64 bits [8]. RC5 is a well-known algorithm developed by the Ron Rivest and a FPGA implementation of RC5 is made with 1787 LUTs with a maximum clock frequency [9] and latest literature shows the implementation of RC5 with 1698 LUTs [10]. RC6 is the modification of RC5 cipher and proven to be more secure when compared RC5 [11]. Some of the lightweight algorithms in the literature are used for mobile devices such as DESL is a light weight crypto with single S box and 1884 GE of power consumption [12]. HIGHT is proposed for low resource environments with RFIDS and sensor devices. Logic utilization of 3086 gates are used for implementation [13]. KATAN comes with various block sizes of 16, 32, and 64 which is suitable for light weight encryption with 802GE of power consumption [14]. And many algorithms are proposed in the literature for light weight encryption. The Tiny encryption algorithm does not have any key generation part, but have simple computational complexity. To overcome this drawback a key generation with 64 bit is proposed, but the key generation consumes more logic. In this work XTEA algorithm with modified key generation is proposed for implementation.

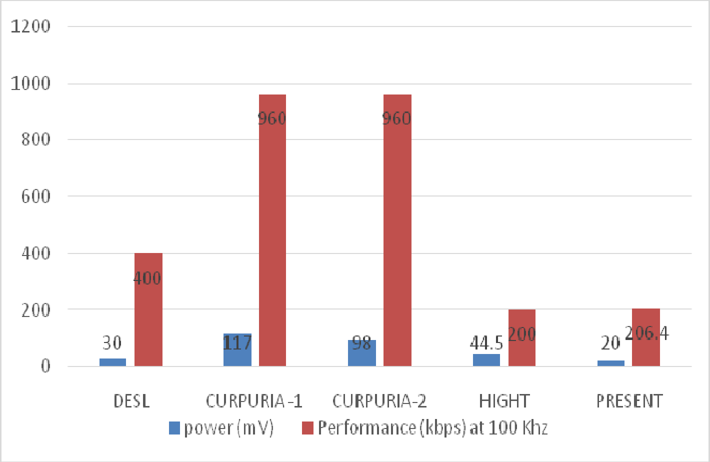

Figure 1: Comparisonof light weight algorithm

3. System Methodology

This work focuses on improving the existing XTEA algorithm. Modified XTEA is a Fiestel-based lightweight block cipher. It is compact towards the hardware implementation. In the original XTEA algorithm, there is no key expansion. Adding a key expansion scheme can make it withstand key differential attacks. Security is based on the number of rounds. The key is a major consideration for the strength of the algorithm, where chaotic map based key sequence generation is proposed in this work.

3.1 Key Generation:

The term “chaotic” represents a state of confusion or disorder and chaotic maps are evolutionary functions that exhibit a chaotic behavior. Chaotic maps are dynamic mathematical system exhibits highly random behavior of the initial condition, which is highly unpredictable, thus even with a small difference in initial conditions will lead to the generation of very different signals from the same dynamical system. The behavior of a chaotic map upon applying initial condition will generate a set of different behaviors for each iteration, which can be taken as a set of key for encrypting data from sensor nodes. Also the natures of chaotic signals are deterministic, reproducible, uncorrelated and random like, which can be very helpful in enhancing the security of transmission in communication. The maps and light weight encryption algorithms are combined as desired, creating keys as complicated as desired. Decryption requires the reverse application of the algorithms.

The chaotic key generates highly random sequence, which can be used for encryption without any process of confusion, as it is already in highly confused state. One dimensional chaotic mapis used for encryption. As the sensor nodes are highly resource constrained battery operated devices performing confusion and diffusion on the text or key should consume less power.

Here one dimensional maps are used for increasing randomness of the key and it will generate a 128 bit master key using this equation 1.

Logistic map equation

$$\boldsymbol{X_{n+1} = rX_n\ (1- X_{n-1}\ )\quad \text{where,}\ \ (r= [3.9, 4)]\ n = [0, 1])} \qquad (1)$$

The equation 1 generates a highly random behavior and it can be depicted from figure 1 and figure 2 gives the key space analysis of the proposed function.

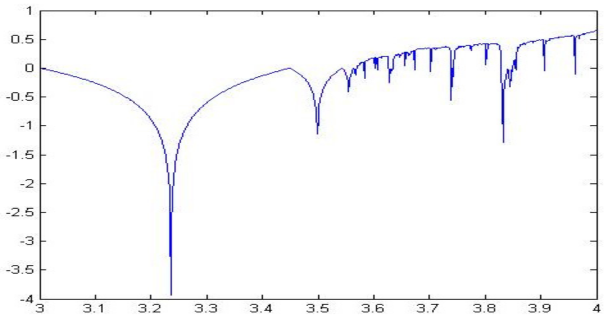

Figure 2: Chaotic map

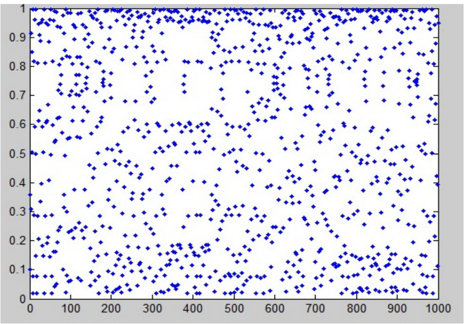

Figure 3: key distribution

3.2 Encryption and decryption:

Modified XTEA needs two w-bit (w=32) words as input, given in two registers X and Y. An expanded key table is used, consisting of t=2*(r+1) words. Initially, left and right shifts are performed on Y register, which are XORed. The result is added with the Y register. Following this, Y is XORed with the ‘S’ array and finally added with the X register. This result is stored in Y register for the next round. Whereas the original value of Y register is stored in X register for the next round. Same process of encryption is reversed for decryption of text.

Algorithm: Light Weight Crypto System

```
Step1: Compute the length of plaintext
Step2: Initialize the iteration and intermediate variable
        i=0; dword1=0; dword2=0; cypher text;
Step3: Pad the plaintext to the nearest multiples of 8
Step4: Encrypt plain text as 64bit (8 char) block
        while (i < plaintext length)
                Pack dword1 with 4bytes by bit shifting in each character
                        No shift for 1 byte, <<8 for 2nd, <<16 for 3rd, <<24 for 4th
                Pack dword2 with 4bytes by bit shifting in each character
                        No shift for 1 byte, <<8 for 2nd, <<16 for 3rd, <<24 for 4th
Step5: Feed dword1 and dword2 as inputs to the traditional TEA Algorithm along with the key.
Step6: Return value of step5 is the cypher text
```

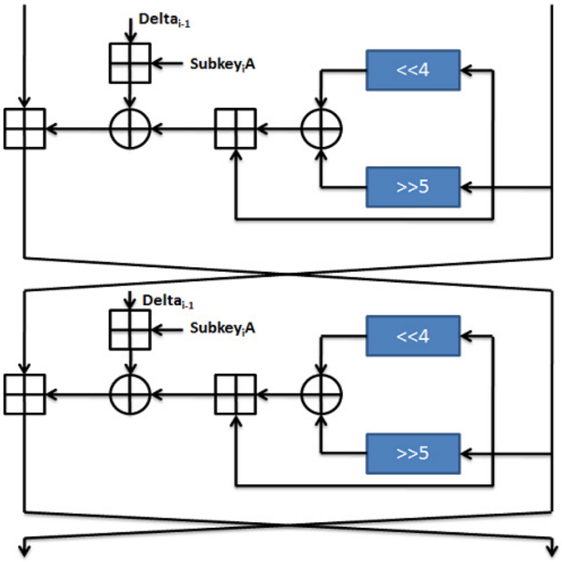

Figure 4: System Model of XTEA

4.Results and discussion:

The proposed algorithm of modified XTEA is done using a Hardware Description Language called Verilog. There are three modules done, one being the key expansion and the other two being encryption and decryption. The algorithm is tested by encrypting and decrypting 128-bit block. The Verilog RTL codes are synthesized to Cyclone II DE 1 FPGA. The implementation results in terms of the logic utilization is tabulated in table 1.

Table1: Implementation Results

Target FPGA Device	Cyclone II
Number of Slices	850
Number of Registers	625
Throughput	200 Mbps
Frequency	50 MHz

The finite state machine implementation of the proposed algorithm is shown in figure 5 and FSM based implementation reduces the logic element consumption and easy debugging with modification. Figure 6 gives the logic space utilization of the proposed algorithm in FPGA.

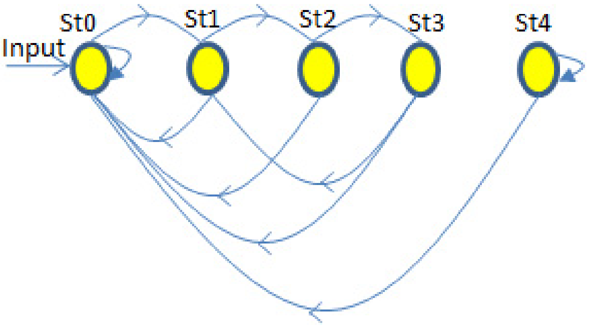

Figure5: Finite state machine implementation

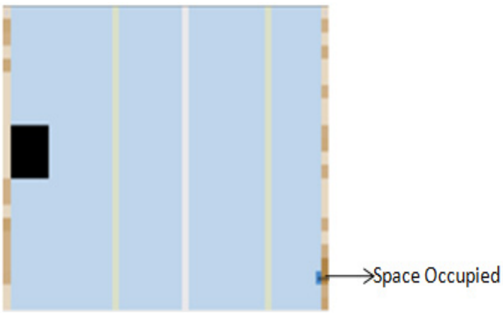

Figure6: Area occupied in the FPGA device

Table 2 gives the comparative analysis of the proposed algorithm with other algorithms available in the literature. The logic utilization of the proposed algorithm is less compared to the other algorithms.

Table2: Comparison analysis

Cipher	Block Size (Bits)	Key Size (Bits)	Throughput (Mbps)	Area	Throughput to Area Ratio
DESL	64	56	400	2762	0.1448
DESXL	64	184	400	3082	0.1297
CURUPIRA-1	96	96	960	8334	0.1151
CURUPIRA-2	96	96	960	7334	0.1308
HIGHT	64	128	200	3901	0.0512
XTEA	64	128	200	3490	0.0573
Proposed Algorithm	64	128	200	1550	0.1290

The proposed algorithm shows better performance in terms of logic utilization, power consumption, area occupied and throughput achieved.

5. Conclusion:

The lightweight encryption algorithm with modified key generation is proposed and implemented in DE1 cyclone II FPGA. The performance of the XTEA algorithm with the chaotic key is analyzed and compared with other traditional lightweight encryption algorithms. The performance in terms of area, throughput and key size is analyzed and better performance is achieved. Lightweight encryption with strong security is achieved using highly randomized chaotic maps based key generation algorithms.

Acknowledgements

The authors wish to express their sincere thanks to the Department of Science & Technology, New Delhi, India (Project ID: SR/FST/ETI-371/2014). We also thank SASTRA University, Thanjavur, India for extending the infrastructural support to carry out this work.

References

1. Good T, Chelton W, Benaissa M. Review of stream cipher candidates from a low resource hardware perspective. ECRYPT eSTREAM; 2006.
2. P.K. Kumar, K. Baskaran. An ASIC implementation of low power and high throughput blowfish crypto algorithm Microelectron J, 41 (2010), pp.7–355
3. Aoki K, Ichikawa T, Kanda M, Matsui M, Moriai S, Nakajima J, & et al. 2000. Specification of Camelia – a 128-bit block cipher. NTT and Mitsubishi Electric Corporation 2000–2001: Nippon Telegraph and Telephone Corporation, Mitsubishi Electric Corporation.
4. Adams C. The CAST-128 encryption algorithm [Online]. Network Working Group available: 〈http://tools.ietf.org/search/rfc2144〉; 1997 B. Roy, W. Meier (Eds.), Fast software encryption, Springer, Berlin, Heidelberg (2004)
5. Adams C, Gilchrist J. The CAST-256 encryption algorithm [Online]. Network Working Group; 1999.
6. Kitsos P, Selimis G, Koufopavlou O, Skodras AN. A hardware implementation of CURUPIRA block cipher for wireless sensors. In: 11th EUROMICRO Conference on Digital System Design Architectures, Methods and Tools, 2008. DSD ′08 ,3–5 September 2008. 2008b. p. 850–3.
7. S. Mangard, F.-X. Standaert (Eds.), Cryptographic hardware and embedded systems, CHES 2010, Springer, Berlin, Heidelberg (2010)
8. H. Feistel, Ibm Block cipher cryptographic system (1971)
9. Rivest RL. The RC5 encryption algorithm. In: Proceedings of the second international workshop on Fast Software Encryption (FSE)

1994, 1994. p. 86–96.

10. D. Koch, M. Korber, J.U. Teich Searching RC5-keys with distributed reconfigurable computing T.P. Plaks (Ed.), ERSA 2006, CSREA Press, Las Vegas, NV, USA (2006), pp. 42–48
11. Riaz M, Heys HM. The FPGA implementation of the RC6 and CAST-256 encryption algorithms. In: Proceedings of the 1999 IEEE Canadian conference on electrical and computer engineering, vol. 1, 9–12 May 1999.p. 367–72.
12. Poschmann A, Leander G, Schramm K, Paar C. New light-weight crypto algorithms for RFID. In: Proceedings of IEEE International Symposium on Circuits and Systems, 2007, ISCAS 2007, 27–30 May 2007. p. 1843–6.
13. Hong D, Sung J, Hong S, Lim J, Lee S, Koo B, et al. HIGHT: a new block cipher suitable for low resource device. In: Proceedings of the 8th international workshop on Cryptographic Hardware and Embedded Systems – CHES 2006. Springer-Verlag Berlin, Heidelberg; 2006.
14. Christophe Cannière, Orr Dunkelman and Miroslav Knežević. KATAN and KTANTAN — a family of small and efficient hardware-oriented block ciphers. In: Proceedings of the 11th international workshop on cryptographic hardware and embedded systems. Lausanne, Switzerland. Springer-Verlag; 2009.